BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-020469

(43)Date of publication of application : 21.01.2000

(51)Int.Cl. G06F 15/00
H04L 9/08
H04L 9/32

(21)Application number : 10-187925

(22)Date of filing : 02.07.1998

(71)Applicant : NEC CORP

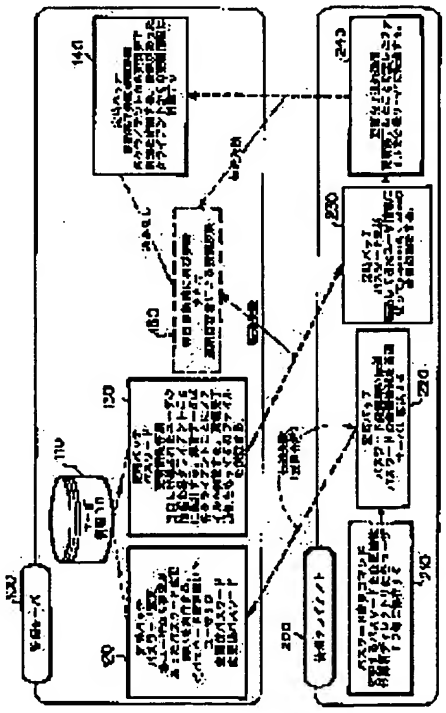
(72)Inventor : FUJIWARA YOHEI

(54) METHOD AND DEVISE FOR MANAGING PASSWORD

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the security of NIS of a UNIX system and to reduce the burden imposed on a managing server.

SOLUTION: Concerning the password managing method for managing a password for permitting the use of data in a network for a user, the method is provided with a managing client 200 for managing the user, a managing server 100 for managing the passwords of all the uses through the respective managing clients 200, and the user information data base for storing the password information of users to be used of the respective managing clients 200. When a user is to update the password, the user inputs the new password to the managing client 200, the managing client 200 stores the former enciphered password and the new enciphered password in pair to the password change request file at fixed time and transfers both the enciphered passwords to the managing server 100, and the managing server 100 performs processing for changing the password of the user while referring to the said user information data base at fixed time.



LEGAL STATUS

[Date of request for examination] 02.07.1998

[Date of sending the examiner's decision of rejection] 26.02.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

JP2000-020469

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the password management method which manages the password for permitting the data use in a user's network The management client which manages a user, and the management server which manages all users' password through said each management client, It has the User Information database which stores a user's password information used by said each management client. In case a user updates a password, a user enters a new password into said management client. Said management client stores the old encryption password and a new encryption password in the file for a password change wish on schedule at a pair. It is the password management method which transmits both the encryption password to said management server, and is characterized by said management server performing processing which changes a user's modification password, referring to said User Information database on schedule.
[Claim 2] It is the password management method characterized by said each management client and said management server performing said password change processing by regular batch processing on schedule in a password management method according to claim 1.
[Claim 3] In the password management method which manages the password for permitting the data use in a user's network In the step which makes a management client the step which sets up one server which performs password management, and other machines, and said each management client The step which performs processing which is not immediately reflected in a system when there is a password change demand by the user, The step which saves password change information per user ID to a password management directory, if it becomes on schedule -- the management server from said each management client -- a password -- changing -- with the step to transmit The step which will process the password change wish transmitted from said each management client, and will check that the password change wish concerned is effective if said management server side also becomes on schedule, The step to which said management server transmits password update information to said each management client, the step which modification of a password will complete by processing the password update information transmitted from said management server in said each management client, and being reflected in said network if it becomes on schedule -- since -- the password management method characterized by becoming.
[Claim 4] The new password information transmitted between said management clients and said management servers in a password management method according to claim 3 is a password management method characterized by not having been enciphered by the standard password function manager for OS, and enciphering using the common cryptographic key managed by said management server and said each management client.
[Claim 5] In the password management equipment which manages the password for permitting the data use in a user's network The management client which manages a user, and the management server which manages all users' password through said management client, It has the User Information database which stores a user's password information used by said each management client. Said management client An input means by which said user enters a new password into said management client, A file memory means to store the old encryption password and a new encryption password in the file for a

password change wish on schedule at a pair, It has a transfer means to transmit said both encryption password to said management server. Said management server A password change processing means to perform processing changed into said new password of said user, referring to said User Information database on schedule, Password management equipment characterized by having a transfer means to transmit the password information of the result depended on said password change processing means to said management client using said both encryption password and a common encryption means.
[Claim 6] It is password management equipment which makes only for managements the encryption new password which said management client enciphered the old password and the new password entered with said input means in password management equipment according to claim 5, respectively, saved, and enciphered the new password, and is characterized by to transmit to said management server by carrying out the encryption old password which enciphered the old password to management.

[Translation done.]

JP2000-020469

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] In a UNIX system, without using NIS (Network Information Service) generally used, this invention aims at improvement in security, and relates to the password management method and password management equipment which perform password management which is used in case two or more machines are operated, and which was put in block.
[0002]
[Description of the Prior Art] Conventionally, it is indicated by JP,60-164859,A as a password management method. This official report is related with the password management method of a distributed-processing computer system. As opposed to what had had and managed the password database according to the individual per conventional computer A local password database is installed in the local computer by which distributed installation was carried out. Share a local computer and to the host computer which carries out a centralized control The host password database which includes all local password databases is installed. It is characterized by registering a password into a host password database and the appointed local password database, respectively, and carrying out common management from the terminal of arbitration connected to this system. In this way, the troublesomeness of the migration procedure of the user by having managed separately for each [which was distributed conventionally] computer of every could be removed, prevention of an unauthorized use of a password could be coped with quickly, and a password registration function manager with big size did not need to be provided for every local, either, and has done so the effectiveness of enabling simplification of the function of a local computer, and mitigation of a load.
[0003] Moreover, the "network user authentication approach" is indicated by JP,8-335207,A, and it is in it. The system chart indicated by this official report is shown and explained to drawing 8 . As shown in drawing 8 , there are some which access each network mutually through a gateway computer. In order to use the resource of such an integrated network, a user needs to prove the justification of his identity to the server which has a user authentication function in each connected network. A log in, a call, and a user offer a password for this actuation to a server, and its identity is proved.
[0004] In drawing 8 , in case a user logs in to a network 1 from the computers 15-16 for users of a network 9, he will mind a gateway computer 11. The security method in such two or more hierarchies' network is a method which judges the existence of the access privilege to other nodes with transmitting the password to each node which the user inputted to the gateway computer 11 of a node used as a direct access place, and a node checking a password.
[0005] The communication media 2 which a network 1 connects each element in a network 1 physically and logically, and turn into a medium of various data transfer, The management computer 3 which performs specially authentication processing of each element and a user which constitutes a network 1, The database 4 for managing the information (ID, password, etc.) about each element and user of a network 1, The authentication courtesy counter 5 which gives a cryptographic key and a log in certificate to a requiring agency according to the demand from each network element and a network

user, With the data base manager 6 which performs read-out and the writing of data from a database 4 The server 7 which offers various services according to the demand from a client 8, the client 8 which communicates with a management computer 3 or a server 7 according to the demand which provides the user of a network 1 with a command interface or an application program, and is emitted by the user through them -- since -- it is constituted.
[0006] Moreover, the network 9 managed independently [a network 1] The communication media 10 which connect physically between each element in nine in a network, and logically, and turn into a medium of various data transfer, The gateway computer 11 with the role which is connected to communication media 2 and 10, transmits the command from the computers 15-16 between users to a network 1, and answers the computer for users in a result, The authentication processing section 12 which transmits an authentication demand to a management computer 3, and performs log in processing to a network 1, The password managed table 13 which manages a gateway computer 11 and the information (ID, password, etc.) about the user of a network 9, the server 14 which offers various services, the computers 15 and 16 for users which communicate according to a demand of the user of a network 9, and the authentication demand section 17 which enters a user's ID and password -- since -- it is constituted.
[0007] Then, if an authentication demand and user ID are transmitted to a management computer 13 from the user computer 15 in the case of a log in, a management computer 13 will be returned to the client for which a user uses the log in certificate enciphered with a user's password, and a cryptographic key. A client 8 decrypts a log in certificate and a cryptographic key with the password which the user entered. In this way, authentication is made possible in a network 1, without a password flowing. Moreover, the user in a network 1 makes authentication possible, without pouring a password to a network 9 similarly, and supposes that unjust acquisition of the password in a gateway computer can be eliminated.
[0008] Moreover, on the other hand, in the UNIX system equipped with a network function as standard, in case user management of two or more machines is performed to a package with NFS (Network File System) of a distributed file system, the so-called NIS (Network Information Service) of an identifier server is used frequently. The centralized control of the identifier of each user on a management server and a password can be performed without troubling the effort of a network administrator making modification of a system reflect for each machine of every by using NIS.
[0009] NIS consists of on a client server model. An NIS server is a host with the NIS data file called a map, and an NIS client is a host who demands such map information.
[0010]
[Problem(s) to be Solved by the Invention] However, there are the following troubles in NIS.
[0011] Since others' password is easily decipherable to it once password information is flying about to the 1st continuously and receives a network top to it like [when changing the time of logging in, and a password], I hear that a problem is in security and it is in it.
[0012] Moreover, since it says at a server an inquiry whenever a client has [2nd] a demand, or a map is transmitted to a slave at any time from a server, I hear that a load is applied to a network and a management server, and it is in them. According to the official report explained in the above-mentioned conventional example, this 2nd trouble is not solved.
[0013] This invention makes it a technical problem to mitigate the burden of a management server while improving the security of NIS of the above-mentioned UNIX system.
[0014]
[Means for Solving the Problem] In the password management method which manages a password for this invention to permit the data use in a user's network The management client which manages a user, and the management server which manages all users' password through said each management client, It has the User Information database which stores a user's password information used by said each management client. In case a user updates a password, a user enters a new password into said management client. Said management client stores the old encryption password and a new encryption password in the file for a password change wish on schedule at a pair. It is characterized by performing

processing which changes a user's modification password, transmitting both the encryption password to said management server, and said management server referring to said User Information database on schedule.

[0015] Moreover, this invention is set to the password management method which manages the password for permitting the data use in a user's network. In the step which makes a management client the step which sets up one server which performs password management, and other machines, and said each management client The step which performs processing which is not immediately reflected in a system when there is a password change demand by the user, The step which saves password change information per user ID to a password management directory, if it becomes on schedule -- the management server from said each management client -- a password -- changing -- with the step to transmit The step which will process the password change wish transmitted from said each management client, and will check that the password change wish concerned is effective if said management server side also becomes on schedule, The step to which said management server transmits password update information to said each management client, the step which modification of a password will complete by processing the password update information transmitted from said management server in said each management client, and being reflected in said network if it becomes on schedule -- since -- it is characterized by becoming.

[0016] Furthermore, this invention is set to the password management equipment which manages the password for permitting the data use in a user's network. The management client which manages a user, and the management server which manages all users' password through said each management client, An input means by which have the User Information database which stores a user's password information used by said each management client, and a user enters a new password into said management client, A file memory means by which said management client stores the old encryption password and a new encryption password in the file for a password change wish on schedule at a pair, They are characterized by having a password change processing means to perform processing which changes a user's modification password, a transfer means to transmit said both encryption password to said management server, and said management server referring to said User Information database, on schedule.

[0017]

[Embodiment of the Invention] The operation gestalt by this invention is explained to a detail, referring to a drawing.

[0018] [The 1st operation gestalt]

(Configuration of this operation gestalt) In drawing 1 , it becomes the management client 200 of WS (WorkStation) which has adopted UNIX, and the management server 100 as an operating system that this method is applicable. With [the number of the management client 200] one [or more], especially the limit is not prepared although the management server 100 consists of one set.

[0019] The password change processing 120 by the regular batch which performs the password change wish which the User Information database DB110 has been arranged and had a demand in the management server 100 from each user, The regular batch password update information creation processing 130 which writes a user's information registered into that day in which total for every client, keep total data to a file for every client, and the file is deleted with the notice of the completion of updating, The notice of the completion of updating is checked from each client, and each processing of the notice check processing 140 of regular batch update completion in which the update information from a client with a notice is deleted is made. Moreover, when you have transfer failure and no notice, updating or compulsive reflection 150 by the operations manager is again processed on the next day at the time of updating.

[0020] Moreover, when the password change command 210 which saves the password to change for every user to the directory for modification information registration is emitted by each management client 200, the password change wish transfer 220 which transmits the modification information on a password to a management server in a regular batch is performed, User Information which has transmitted in a regular batch follows, and it is password. The renewal 230 of a password carry out the

modification processing of shadow is performed, and the notice transfer 240 of the completion of updating is performed to a management server.
[0021] Since the management server and management client by this operation gestalt performed updating and management processing of a password, an expression called a management server and a management client was especially used for them, but even if it is a general server and a client, since they can attain the configuration, and actuation and an operation of this operation gestalt, they do not adhere to the name.
[0022] (Actuation of this operation gestalt) Next, actuation of this whole operation gestalt is explained to a detail with reference to drawing 2 . By the UNIX system, when a password is generated in a transmission line, since it is a phase and a time of changing a password, the actuation at the time of a password change is explained at the beginning which registers self identifier and password when wishing entry to a system.
[0023] First, in each management client 200, a user executes the password change command 210 prepared for these methods. The password enciphered from the password entry of each management client (trypt) is extracted (211). The password before the user itself changing into the next is entered (212). Compare this enciphered password with the entered password (213), and a user check will be ended if in agreement. Enter a new password twice for a check (214), and the file for a password change wish is created. The new password enciphered as the enciphered old password is saved (215), a new password is enciphered, it carries out only to managements, the entered old password is enciphered, and it transmits to (216) and the management server 100 as an object for management.
[0024] The file for a password change wish is created for every user ID by executing this command. The new password and the old password which were enciphered by the exclusive cryptographic key are saved at this file. If this file becomes on schedule every day, it will be transmitted to a management server (management client password change command 210 of drawing 2).
[0025] Next, by the management server 100, as shown in drawing 2 , if it becomes on schedule every day, password change processing will be performed (120). The new password which read each transmitted file for a password change wish, and was enciphered as the enciphered old password is read (121), the password of User Information DB110 is compared with the sent old password (122), and if equal, a new password (what was enciphered by the exclusive cryptographic key) is registered and (123) stored in User Information DB110 (password change processing 120 of the management server of drawing 2).
[0026] Next, in the management server 100, if it becomes on schedule every day, as user update information creation processing 130, a password change will be read from User Information DB110 (161), and the updated list list which bundled up the password with which it was enciphered only for [on User Information DB110] managements will be written in the file for a transfer (162). It is transmitted to each management client 200 which corresponds this user update information (163).
[0027] When it becomes on schedule every day, the transmitted user update information file is read and compound-ized (231), and the password registered on User Information DB110 is made to reflect in a system by each management client 200 finally (management client User Information update process 230 of drawing 2).
[0028] Next, each processing is explained concretely.
[0029] With reference to drawing 4 , the password change command 210 prepared for each management client 200 is explained first. If this command is executed, the input of a current password will be required (211) and a current password will be entered (212). If the entered password and the password registered into /etc/shadow are equal (213), the input of a new password will be required twice (214,214'). If a new password is the same twice [both] (215), the old password and a new password will be written in a password change wish file (217), and a password will be enciphered by the cryptographic key only for managements (218). The enciphered password is transmitted to a management server. on the other hand -- step 213,215 -- it is -- etc. -- it spreads -- twisting -- a case -- steps 21A and 21B -- password coincidence -- not carrying out -- ****** -- warning [like] is emitted and it ends.

[0030] Next, with reference to drawing 5 , the password change wish transfer processing 220 is explained. If it becomes on schedule every day, the password change wish file for every user under a password management directory will be searched with each management client 200 (221), and a password change file will be altogether transmitted to the management server 100 using the rcp command (222). It judges whether it succeeded in the transfer (223), and the password change wish file on each management client is deleted after checking a transfer success (224). When a transfer goes wrong at step 223, processing again transmitted at the time of next starting is performed.
[0031] Next, with reference to drawing 3 , the password change processing 120 on the management server 100 is explained. In the management server 100, if it becomes on schedule every day, the password change wish file 220 transmitted from each management client will be processed. First, the list of files in a password management directory is created, and it processes it one [at a time] (121). Next, the old password and a new password are read from the password information file 111 (122). Next, the password on User Information DB110 is read (123). About each file, if the password on User Information DB110 and the old password on a file are equal (124), a new password is made to reflect on User Information DB110, and is stored (125). (status: password change) Otherwise, the electronic mail of the purport which is an abnormal condition is transmitted to a user with a request, and addressing to a management server operator (128), and status on the user D information B is changed into "password update failed" (129). The transmitted file is deleted after these processings are completed (126). The above-mentioned processing is repeated for every user (127).
[0032] Next, with reference to drawing 6 , the user update information creation processing 130 on the management server 100 is explained. If it becomes on schedule in the management server 100 every day, all users' update information will be checked on User Information DB110 (131). Search a list with renewal of a password and it judges whether the flag of the updated purport is ON (132). every corresponding registration place -- a use situation -- checking (133) -- status of a use situation -- a password change -- or it judging whether it is one of the password update failed (134), and, if it is a password change It creates in the form where a user update information file is Append(ed) as a transfer file of the corresponding registration place (135). This is processed for every registration place, if all registration places are checked (137) and it ends, an update flag will be cleared (138), and it judges whether all users' check was ended (139), and ends.
[0033] Finally, with reference to drawing 7 , the renewal 230 of User Information on the management client 200 is explained. In each management client 200, if it becomes on schedule every day, it will start as a regular batch and the information transmitted from the management server 100 once [1] per day will be processed. The management client 200 searches the transmitted User Information update file (234), processes it sequentially according to the contents of the user update information file, and is read from the pointer of a file by one line (235). Next, a setup of a management client is changed into the password shown from the management server 100 (236). The additional writing of the updating result is carried out at the notice file of updating (237). Next it confirms whether reading was ended to the last of a user update information file (238), and the notice file of updating is transmitted to a management server (239). In this way, if modification of a password is checked, it will be written in the notice file of updating, and the notice file of updating will be transmitted to a management server after completing all processings (239).
[0034] In drawing 1 , as mentioned above, in order that the management client 200 may update a password on schedule, it performs modification processing of a password according to transmitted User Information (230), and transmits the file which described having carried out the completion of updating of this result for the notice transmission of the completion of updating to the management server 100 as regular batch processing, (240). In a management server, the notice of the completion of updating is checked from each management client 200 as notice check processing of the completion of updating of regular batch processing. Then, the update information from a management client with a notice is deleted. In this way, a series of batch processing is ended (140). Here, when a transfer goes wrong, in the management server 100, regular batch processing is made at the next day, for example, re-transfer directions are carried out at a management client at the compulsive target by ** or the operations

manager, and the completion processing of updating is performed (150).
[0035]
[Effect of the Invention] Since according to this invention password information was enciphered and it has transmitted on a network using the cryptographic key of the dedication which shared between a management server and each management client, and has been managed, it is in being easily undecipherable even if the password information file under transfer includes others' hand. Consequently, the security of a system improves.
[0036] Moreover, since a centralized control is carried out on a management server, the package management of the management client which are two or more UNIX machines can be carried out. Consequently, the effort in a system management mitigates.
[0037] Furthermore, since on time ** does not have the information transfer between a management server and each management client and it is performed every day using a regular batch, the traffic which flows a network top can be mitigated and the load of a management server and each management client can be mitigated. Consequently, the load to a network mitigates.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－20469
（P2000－20469A）
(43)公開日　平成12年１月21日(2000.1.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｚ	５Ｋ０１３
9/32			６７３Ａ	

審査請求　有　請求項の数６　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－187925

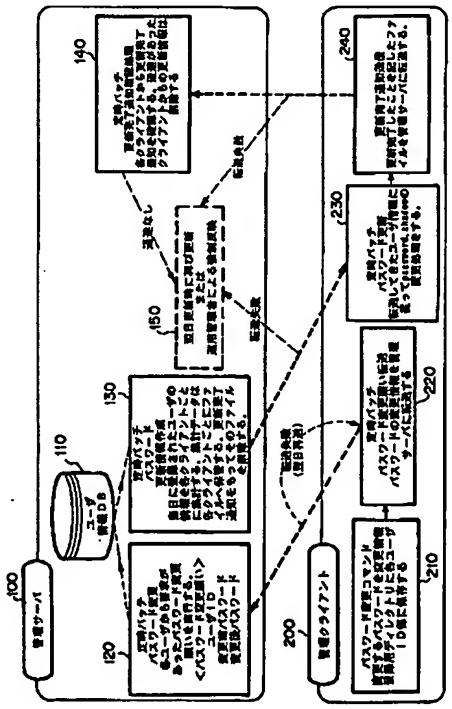
(22)出願日　平成10年７月２日(1998.7.2)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　冨士原　洋平
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100065385
弁理士　山下　穣平

Ｆターム(参考)　5B085 AC05 AE02 AE03 AE09 BA02
5K013 AA01 BA02 GA00 GA04

(54)【発明の名称】　パスワード管理方法とその装置

(57)【要約】
【課題】　ＵＮＩＸシステムのＮＩＳのセキュリティを向上すると共に、管理サーバの負担を軽減することを課題とする。
【解決手段】　ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、ユーザを管理する管理クライアントと、前記各管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、ユーザがパスワードを更新する際、ユーザは新パスワードを前記管理クライアントに入力し、前記管理クライアントは定時にパスワード変更願い用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納し、両暗号化パスワードを前記管理サーバに転送し、前記管理サーバは定時に前記ユーザ情報データベースを参照しつつユーザの変更パスワードを変更する処理を行うことを特徴とする。



【特許請求の範囲】
【請求項1】 ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、
ユーザを管理する管理クライアントと、前記各管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、
ユーザがパスワードを更新する際、ユーザは新パスワードを前記管理クライアントに入力し、前記管理クライアントは定時にパスワード変更願い用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納し、両暗号化パスワードを前記管理サーバに転送し、前記管理サーバは定時に前記ユーザ情報データベースを参照しつつユーザの変更パスワードを変更する処理を行うことを特徴とするパスワード管理方法。
【請求項2】 請求項1に記載のパスワード管理方法において、前記各管理クライアント及び前記管理サーバは、定時に定時バッチ処理により前記パスワード変更処理を行うことを特徴とするパスワード管理方法。
【請求項3】 ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、
パスワード管理を行うサーバを一台設定するステップと、
他のマシンは管理クライアントとするステップと、
前記各管理クライアントにおいて、ユーザによりパスワード変更要求があったときシステムにすぐ反映しない処理を行うステップと、
パスワード管理ディレクトリにユーザＩＤ単位にパスワード変更情報を保存するステップと、
定時になると前記各管理クライアントから管理サーバにパスワードの変更願いが転送するステップと、
前記管理サーバ側も定時になると前記各管理クライアントから転送されてきたパスワード変更願いを処理して当該パスワード変更願いが有効であることを確認するステップと、
前記管理サーバが前記各管理クライアントに対してパスワード更新情報を転送するステップと、
定時になると前記各管理クライアントでは前記管理サーバから転送されたパスワード更新情報を処理し前記ネットワークに反映することによりパスワードの変更が完了するステップと、からなることを特徴とするパスワード管理方法。
【請求項4】 請求項3に記載のパスワード管理方法において、
前記管理クライアントと前記管理サーバ間で転送される新パスワード情報はＯＳ標準のパスワード管理機能により暗号化されたものではなくて、前記管理サーバ及び前記各管理クライアントで管理している共通の暗号化キーを用いて暗号化したものであることを特徴とするパスワード管理方法。
【請求項5】 ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理装置において、
ユーザを管理する管理クライアントと、前記管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、
前記管理クライアントは、前記ユーザは新パスワードを前記管理クライアントに入力する入力手段と、
定時にパスワード変更願い用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納するファイル記憶手段と、
前記両暗号化パスワードを前記管理サーバに転送する転送手段と、を備え、
前記管理サーバは、定時に前記ユーザ情報データベースを参照しつつ前記ユーザの前記新パスワードに変更する処理を行うパスワード変更処理手段と、
前記パスワード変更処理手段による結果のパスワード情報を前記両暗号化パスワードと共通の暗号化手段を用いて前記管理クライアントに転送する転送手段と、を備えたことを特徴とするパスワード管理装置。
【請求項6】 請求項5に記載のパスワード管理装置において、
前記管理クライアントは、前記入力手段で入力した旧パスワードと新パスワードとをそれぞれ暗号化して保存し、新パスワードを暗号化した暗号化新パスワードを管理専用とし、旧パスワードを暗号化した暗号化旧パスワードを管理用として、前記管理サーバに転送することを特徴とするパスワード管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＵＮＩＸシステムにおいて、一般に利用されているＮＩＳ（Network Information Service）を使用せずに、セキュリティの向上を図り、複数マシンを操作する際に用いる一括したパスワード管理を行うパスワード管理方法及びパスワード管理装置に関する。
【０００２】
【従来の技術】従来、パスワード管理方式として、特開昭６０－１６４８５９号公報に開示されている。本公報は、分散処理コンピュータシステムのパスワード管理方式に関し、従来のコンピュータ単位で個別にパスワードデータベースを有して管理していたものに対し、分散設置されたローカルコンピュータにローカルパスワードデータベースを設置し、ローカルコンピュータを共有し、集中管理するホストコンピュータに、全てのローカルパ

スワードデータベースを包括するホストパスワードデータベースを設置し、該システムに接続される任意の端末よりパスワードをホストパスワードデータベースならびに指定のローカルパスワードデータベースにそれぞれ登録し、共通管理することを特徴としている。こうして、従来分散した各コンピュータ毎に別々に管理していたことによる使用者の移動手続の煩わしさを除去でき、パスワードの不正使用の防止に迅速に対処でき、サイズの大きなパスワード登録管理機能も、ローカル毎に具備する必要もなく、ローカルコンピュータの機能の簡素化と負荷の軽減を可能とするという効果を奏している。

【０００３】また、特開平８－３３５２０７号公報に「ネットワークユーザ認証方法」が開示されいる。図８に該公報に記載されたシステム図を示して説明する。図８に示すように、ゲートウエイコンピュータを介して各ネットワークを相互にアクセスするものがある。このような統合ネットワークの資源を利用するために、ユーザは接続された各ネットワーク中のユーザ認証機能を有するサーバに対して自分の身元の正当性を証明する必要がある。この動作をログインと呼び、ユーザはサーバに対してパスワードを提供して自分の身元を証明する。

【０００４】図８において、ユーザはネットワーク９のユーザ用コンピュータ１５～１６からネットワーク１へログインする際に、ゲートウエイコンピュータ１１を介することとなる。このような２階層以上のネットワークにおけるセキュリティ方式は、ユーザが入力した各ノードへのパスワードを、直接のアクセス先となるノードのゲートウエイコンピュータ１１に送信し、ノードがパスワードをチェックすることで他のノードへのアクセス権の有無を判断する方式である。

【０００５】ネットワーク１は、ネットワーク１内の各要素を物理的・論理的に接続し各種データ転送の媒体となる通信媒体２と、ネットワーク１を構成する各要素やユーザの認証処理を専門に行う管理コンピュータ３と、ネットワーク１の各要素やユーザに関する情報（ＩＤ、パスワード等）を管理するためのデータベース４と、ネットワークの各要素やユーザからの要求に応じて暗号鍵やログイン証明書を要求元に与える認証サービス部５と、データベース４からデータの読み出しや書き込みを行うデータベース管理部６と、クライアント８からの要求に応じて各種サービスを提供するサーバ７と、ネットワーク１のユーザにコマンドインターフェースやアプリケーションプログラムを提供しそれらを通じてユーザから発せられる要求に応じて管理コンピュータ３やサーバ７と通信を行うクライアント８と、から構成されている。

【０００６】また、ネットワーク１とは独立に管理されるネットワーク９は、ネットワーク内９内の各要素間の物理的・論理的に接続し各種データ転送の媒体となる通信媒体１０と、通信媒体２と１０に接続されユーザ間コンピュータ１５～１６からのコマンドをネットワーク１に送信し結果をユーザ用コンピュータに返信する役割をもつゲートウエイコンピュータ１１と、管理コンピュータ３に認証要求を送信してネットワーク１へのログイン処理を行う認証処理部１２と、ゲートウエイコンピュータ１１及びネットワーク９のユーザに関する情報（ＩＤ、パスワード等）を管理するパスワード管理テーブル１３と、各種サービスを提供するサーバ１４と、ネットワーク９のユーザの要求に応じて通信するユーザ用コンピュータ１５，１６と、ユーザのＩＤやパスワードを入力する認証要求部１７と、から構成されている。

【０００７】そうして、ログインの際、ユーザコンピュータ１５から管理コンピュータ１３に認証要求とユーザＩＤを送信すると、管理コンピュータ１３はユーザのパスワードで暗号化したログイン証明書と暗号鍵をユーザが使用するクライアントに返す。クライアント８はユーザが入力したパスワードによりログイン証明書と暗号鍵を復号化する。こうして、ネットワーク１にはパスワードが流れずに認証を可能とする。また、ネットワーク１内のユーザは、同様にネットワーク９にパスワードを流さずに認証を可能とし、ゲートウエイコンピュータにおけるパスワードの不正入手を排除できるとしている。

【０００８】また一方、ネットワーク機能を標準で備えるＵＮＩＸシステムにおいて、分散ファイルシステムのＮＦＳ（Network File System）と共に、複数マシンのユーザ管理を一括に行う際はいわゆる名前サーバのＮＩＳ（Network Information Service）が頻繁に使用されている。ＮＩＳを使用することにより、ネットワーク管理者は個々のマシン毎にシステムの変更を反映させるといった労力を煩わせることなく、管理サーバ上での各ユーザの名前とパスワードとの集中管理が行える。

【０００９】ＮＩＳはクライアント・サーバモデル上で構成される。ＮＩＳサーバとは、マップと呼ばれるＮＩＳデータファイルを持つホストのことで、ＮＩＳクライアントとは、これらのマップ情報を要求するホストのことである。

【００１０】

【発明が解決しようとする課題】しかし、ＮＩＳには、次のような問題点がある。

【００１１】第１に、ログインする際やパスワードを変更するときのように、パスワード情報がネットワーク上を絶えず飛び交っており、いったん入手すれば他人のパスワードを容易に解読出来るので、セキュリティに問題があるということである。

【００１２】また、第２に、クライアントが要求のある度にサーバに問い合わせにいったり、サーバからスレーブにマップが随時転送されるので、ネットワーク、管理サーバに負荷がかかるということである。上述の従来例で説明した公報によれば、この第２の問題点を解決していない。

【００１３】本発明は、上記ＵＮＩＸシステムのＮＩＳのセキュリティを向上すると共に、管理サーバの負担を軽減することを課題とする。

【００１４】

【課題を解決するための手段】本発明は、ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、ユーザを管理する管理クライアントと、前記各管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、ユーザがパスワードを更新する際、ユーザは新パスワードを前記管理クライアントに入力し、前記管理クライアントは定時にパスワード変更願い用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納し、両暗号化パスワードを前記管理サーバに転送し、前記管理サーバは定時に前記ユーザ情報データベースを参照しつつユーザの変更パスワードを変更する処理を行うことを特徴とする。

【００１５】また、本発明は、ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理方法において、パスワード管理を行うサーバを一台設定するステップと、他のマシンは管理クライアントとするステップと、前記各管理クライアントにおいて、ユーザによりパスワード変更要求があったときシステムにすぐ反映しない処理を行うステップと、パスワード管理ディレクトリにユーザＩＤ単位にパスワード変更情報を保存するステップと、定時になると前記各管理クライアントから管理サーバにパスワードの変更願いが転送するステップと、前記管理サーバ側も定時になると前記各管理クライアントから転送されてきたパスワード変更願いを処理して当該パスワード変更願いが有効であることを確認するステップと、前記管理サーバが前記各管理クライアントに対してパスワード更新情報を転送するステップと、定時になると前記各管理クライアントでは前記管理サーバから転送されたパスワード更新情報を処理し前記ネットワークに反映することによりパスワードの変更が完了するステップと、からなることを特徴とする。

【００１６】更に、本発明は、ユーザのネットワーク内のデータ使用を許可するためのパスワードを管理するパスワード管理装置において、ユーザを管理する管理クライアントと、前記各管理クライアントを通じて全ユーザのパスワードを管理する管理サーバと、前記各管理クライアントで使用するユーザのパスワード情報を格納するユーザ情報データベースとを備え、ユーザは新パスワードを前記管理クライアントに入力する入力手段と、前記管理クライアントは定時にパスワード変更願い用ファイルに旧暗号化パスワードと新暗号化パスワードとを対に格納するファイル記憶手段と、前記両暗号化パスワードを前記管理サーバに転送する転送手段と、前記管理サーバは定時に前記ユーザ情報データベースを参照しつつユーザの変更パスワードを変更する処理を行うパスワード変更処理手段と、を備えたことを特徴とする。

【００１７】

【発明の実施の形態】本発明による実施形態について、図面を参照しつつ詳細に説明する。

【００１８】［第１の実施形態］

（本実施形態の構成）図１において、本方式を適用できるのはオペレーティングシステムとして、ＵＮＩＸを採用しているＷＳ（WorkStation）の管理クライアント２００と、管理サーバ１００となる。管理サーバ１００は一台から構成されるが、管理クライアント２００の台数は１以上であれば、制限は特に設けていない。

【００１９】管理サーバ１００には、ユーザ情報データベースＤＢ１１０が配置され、各ユーザから要求があったパスワード変更願いを実行する定時バッチによるパスワード変更処理１２０と、当日に登録されたユーザの情報を書くクライアントごとに集計し、集計データは各クライアント毎にファイルへ保管し、更新完了通知をもってそのファイルを削除する定時バッチパスワード更新情報作成処理１３０と、各クライアントから更新完了通知を確認し、通知があったクライアントからの更新情報は削除する定時バッチ更新完了通知確認処理１４０の各処理がなされる。また、転送失敗や通知なしの場合に翌日更新時に再び更新又は運用管理者による強制反映１５０の処理を行う。

【００２０】また、各管理クライアント２００には、変更するパスワードを変更情報登録用ディレクトリに各ユーザ毎に保存するパスワード変更コマンド２１０が発せられると、定時バッチでパスワードの変更情報を管理サーバに転送するパスワード変更願い転送２２０が実行され、定時バッチで転送してきたユーザ情報に従ってpassword shadowの変更処理をするパスワード更新２３０が実行され、更新完了通知転送２４０が管理サーバに対して実行される。

【００２１】本実施形態による管理サーバや管理クライアントは、パスワードの更新及び管理処理を実行するので、特に管理サーバや管理クライアントという表現を用いたが、一般のサーバやクライアントであっても、本実施形態の構成及び動作・作用を達成できるので、その名称に拘ることはない。

【００２２】（本実施形態の動作）次に、図２を参照して、本実施形態の全体の動作について詳細に説明する。ＵＮＩＸ系システムでは、パスワードが伝送ラインに発生する場合は、システムへの参入を希望するときの自己の名前とパスワードを登録する当初段階と、パスワードを変更するときであるので、パスワード変更時における動作について説明する。

【００２３】まず、各管理クライアント２００におい

て、ユーザが、本方式用に用意されたパスワード変更コマンド２１０を実行する。各管理クライアントのパスワードエントリから暗号化（trypt）されたパスワードを抽出する（２１１）。つぎに、ユーザ自身が変更前のパスワードを入力する（２１２）。この暗号化されたパスワードと入力したパスワードとを比較し（２１３）、一致しておればユーザ確認を終了して、新しいパスワードを確認のため２回入力し（２１４）、パスワード変更願い用ファイルを作成し、暗号化した旧パスワードと暗号化した新パスワードとを保存し（２１５）、新パスワードを暗号化して管理専用とし、入力した旧パスワードを暗号化して管理用として（２１６）、管理サーバ１００に転送する。

【００２４】このコマンドを実行することによりパスワード変更願い用ファイルがユーザＩＤ毎に作成される。このファイルには専用暗号化キーで暗号化された新パスワードと旧パスワードが保存される。このファイルは毎日定時になると管理サーバに転送される（図２の管理クライアント・パスワード変更コマンド２１０）。

【００２５】次に、図２に示すように、管理サーバ１００では毎日定時になると、パスワード変更処理を実行する（１２０）。転送されてきた各パスワード変更願い用ファイルを読み込み、暗号化された旧パスワードと暗号化された新パスワードとを読み込み（１２１）、ユーザ情報ＤＢ１１０のパスワードと送られてきた旧パスワードを比較し（１２２）、等しければ新パスワード（専用暗号化キーで暗号化されたもの）をユーザ情報ＤＢ１１０に登録して（１２３）、格納する（図２の管理サーバのパスワード変更処理１２０）。

【００２６】次に、管理サーバ１００では毎日定時になると、ユーザ更新情報作成処理１３０として、ユーザ情報ＤＢ１１０からパスワード変更を読み込み（１６１）、ユーザ情報ＤＢ１１０上の管理専用の暗号化されたパスワードを一括した更新されたリスト一覧を転送用ファイルに書き込む（１６２）。このユーザ更新情報を該当する各管理クライアント２００へ転送される（１６３）。

【００２７】最後に、各管理クライアント２００では毎日定時になると、転送されてきたユーザ更新情報ファイルを読み込み、複合化して（２３１）、ユーザ情報ＤＢ１１０上に登録されているパスワードをシステムに反映させる（図２の管理クライアントユーザ情報更新処理２３０）。

【００２８】次に、各処理について具体的に説明する。

【００２９】まず図４を参照して、各管理クライアント２００に用意するパスワード変更コマンド２１０について説明する。このコマンドを実行すると、現在のパスワードの入力を要求され（２１１）、現在のパスワードを入力する（２１２）。入力したパスワードと/etc/shadowに登録されているパスワードが等しければ（２１３）、新しいパスワードの入力が２回要求される（２１４，２１４’）。新しいパスワードが２回共に同じであれば（２１５）、パスワード変更願いファイルに旧パスワードと新パスワードが書き込まれ（２１７）、パスワードは管理専用暗号化キーで暗号化する（２１８）。暗号化されたパスワードは管理サーバに転送される。一方、ステップ２１３，２１５で等しくない場合には、ステップ２１Ａ，２１Ｂで、パスワード一致せずというような警告を発して終了する。

【００３０】次に、図５を参照して、パスワード変更願い転送処理２２０について説明する。毎日定時になると、各管理クライアント２００ではパスワード管理ディレクトリ下にあるユーザ毎のパスワード変更願いファイルを検索し（２２１）、パスワード変更ファイルを全てrcpコマンドを用いて管理サーバ１００に転送する（２２２）。転送に成功したか否かを判断し（２２３）、転送成功を確認後、各管理クライアント上のパスワード変更願いファイルを削除する（２２４）。ステップ２２３で転送に失敗した場合には、次回の起動時に再度転送する処理を行う。

【００３１】次に、図３を参照して、管理サーバ１００上でのパスワード変更処理１２０について説明する。管理サーバ１００では、毎日定時になると、各管理クライアントから転送されてきたパスワード変更願いファイル２２０を処理する。まず、パスワード管理ディレクトリにあるファイルのリストを作成し、一つずつ処理する（１２１）。つぎに、パスワード情報ファイル１１１から旧パスワードと新パスワードとを読み込む（１２２）。次にユーザ情報ＤＢ１１０上のパスワードを読み込む（１２３）。各ファイルについて、ユーザ情報ＤＢ１１０上のパスワードとファイル上の旧パスワードが等しければ（１２４）、新パスワードをユーザ情報ＤＢ１１０上に反映させて（status：パスワード変更）格納する（１２５）。そうでなければ依頼のあったユーザと管理サーバオペレータ宛に異常状態である旨の電子メールを送信し（１２８）、ユーザD情報B上のｓｔａｔｕｓを「パスワード更新失敗」に変更する（１２９）。これらの処理が終了した後に、転送されてきたファイルを削除する（１２６）。各ユーザ毎に上記処理を繰り返す（１２７）。

【００３２】次に図６を参照して、管理サーバ１００上でのユーザ更新情報作成処理１３０について説明する。管理サーバ１００では毎日定時になると、ユーザ情報ＤＢ１１０上で全ユーザの更新情報をチェックし（１３１）、パスワード更新のあったリストを検索し、更新した旨のフラグがＯＮであるかどうかを判断し（１３２）、該当する登録先毎に利用状況をチェックし（１３３）、利用状況のstatusがパスワード変更か又はパスワード更新失敗のどれかであるかを判断し（１３４）、パスワード変更であれば、該当する登録先の転送ファイル

としてユーザ更新情報ファイルをAppendする形で作成する（１３５）。これを登録先毎に処理し、全登録先をチェックし（１３７）、終了すれば更新フラグをクリアーし（１３８）、全ユーザのチェックを終了したかを判断し（１３９）、終了する。

【００３３】最後に、図7を参照して、管理クライアント２００上でのユーザ情報更新２３０について説明する。各管理クライアント２００では毎日定時になると、定時バッチとして起動し、１日１回管理サーバ１００から転送されてくる情報を処理する。管理クライアント２００は、転送されてきたユーザ情報更新ファイルを検索し（２３４）、ユーザ更新情報ファイルの内容に従って順次処理していき、ファイルのポインタから１行分読み込む（２３５）。つぎに、管理サーバ１００から提示されたパスワードに管理クライアントの設定を変更する（２３６）。更新結果を更新通知ファイルに追加書き込みする（２３７）。つぎに、ユーザ更新情報ファイルの最後まで読み込みを終了したかをチェックし（２３８）、更新通知ファイルを管理サーバに送信する（２３９）。こうして、パスワードの変更が確認されたら、更新通知ファイルに書き込まれ、全ての処理が終了後、更新通知ファイルは管理サーバに転送される（２３９）。

【００３４】上述したように、図1において、管理クライアント２００は、定時バッチ処理として、定時にパスワードを更新するため、転送されてきたユーザ情報に従ってパスワードの変更処理を行い（２３０）、この結果を更新完了通知送信のため、更新完了したことを記述したファイルを管理サーバ１００に転送する（２４０）。管理サーバでは、定時バッチ処理の更新完了通知確認処理として、各管理クライアント２００から更新完了通知を確認する。その後、通知のあった管理クライアントからの更新情報は削除する。こうして一連のバッチ処理を終了する（１４０）。ここで、転送を失敗したときには、管理サーバ１００では、例えば翌日に定時バッチ処理がなされか、または運用管理者による強制的に管理クライアントに再転送指示して更新完了処理を実行する（１５０）。

【００３５】

【発明の効果】本発明によれば、管理サーバ、及び各管理クライアントで共有して管理している専用の暗号化キーを利用して、パスワード情報を暗号化してネットワーク上に転送しているので、転送中のパスワード情報ファイルが他人の手に渡っても容易に解読出来ないことにある。この結果、システムのセキュリティが向上する。

【００３６】また、管理サーバ上で集中管理するため、複数のＵＮＩＸマシンである管理クライアントを一括管理できる。この結果、システム管理における労力が軽減する。

【００３７】さらに、管理サーバと各管理クライアント間での情報転送が、オンタイムではなくて、毎日定時バッチを用いて行われるため、ネットワーク上を流れるトラフィックを軽減でき、管理サーバと各管理クライアントの負荷を軽減できる。この結果、ネットワークへの負荷が軽減する。

【図面の簡単な説明】

【図１】本発明の実施形態によるパスワード管理機能の概要図である。

【図２】本発明の実施形態によるパスワード管理の流れ図である。

【図３】本発明の実施形態による管理サーバのパスワード変更処理のフローチャートである。

【図4】本発明の実施形態による管理クライアントのパスワード変更コマンド処理のフローチャートである。

【図5】本発明の実施形態による管理クライアントのパスワード変更願い転送処理のフローチャートである。

【図6】本発明の実施形態による管理サーバのユーザ更新情報作成処理のフローチャートである。

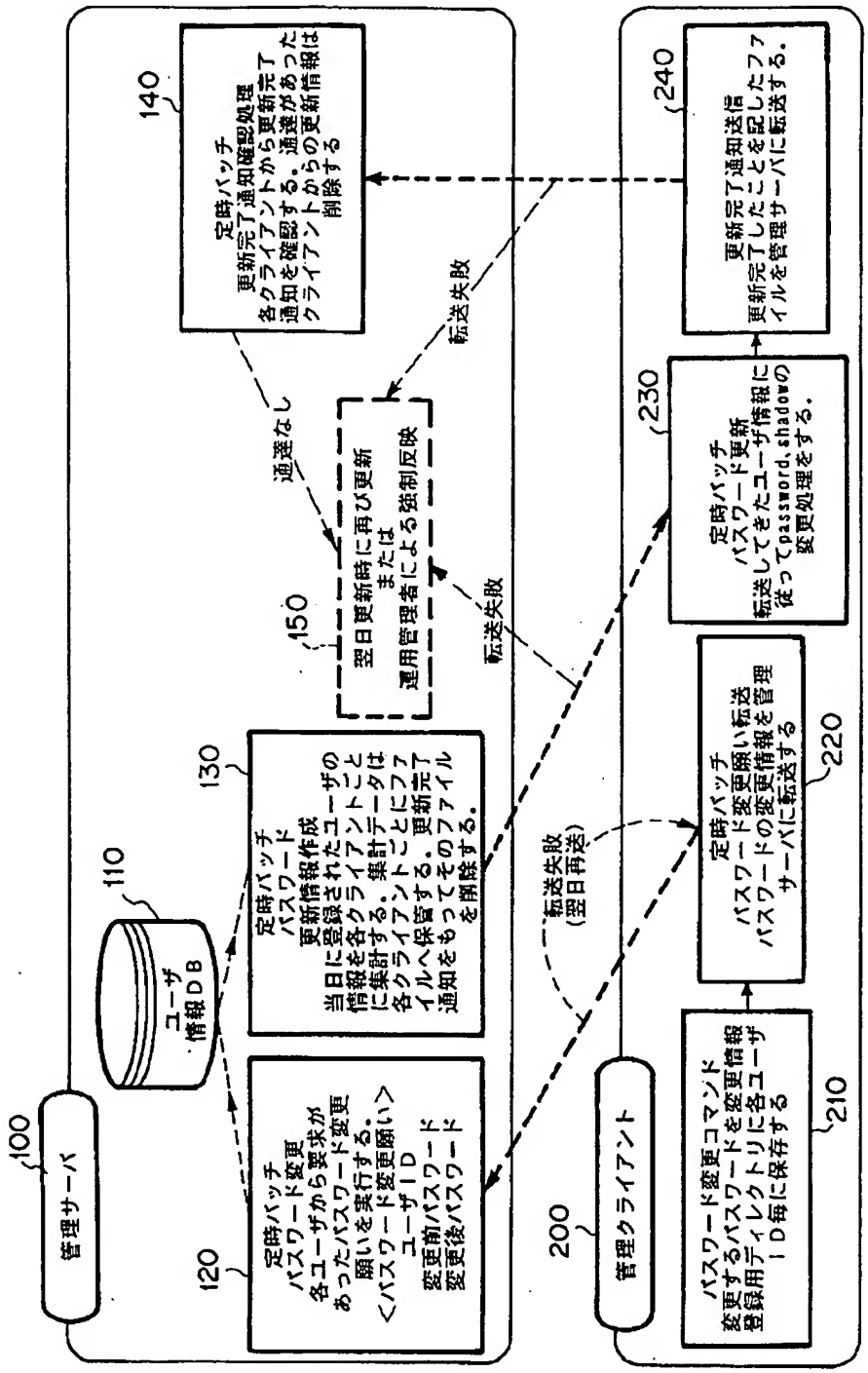
【図7】本発明の実施形態による管理クライアントのユーザ更新情報処理のフローチャートである。

【図8】従来のネットワーク認証方法によるシステム概略図である。

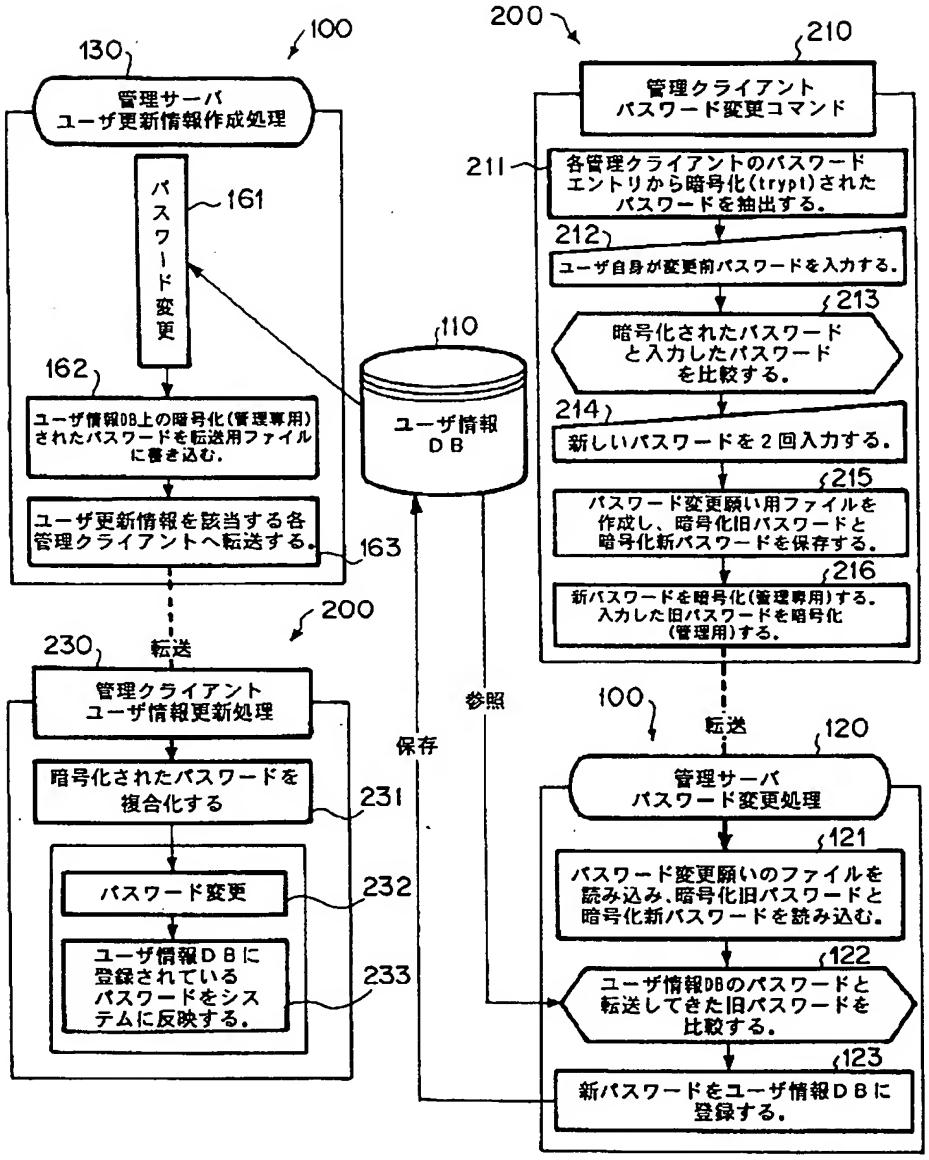
【符号の説明】

１００　管理サーバ
１１０　ユーザ情報データベース
１２０　定時バッチパスワード変更処理
１３０　定時バッチパスワード処理
１４０　定時バッチ更新完了通知確認処理
２００　管理クライアント
２１０　パスワード変更コマンド
２２０　定時バッチパスワード変更願い転送処理
２３０　定時バッチパスワード更新処理
２４０　更新完了通知確認

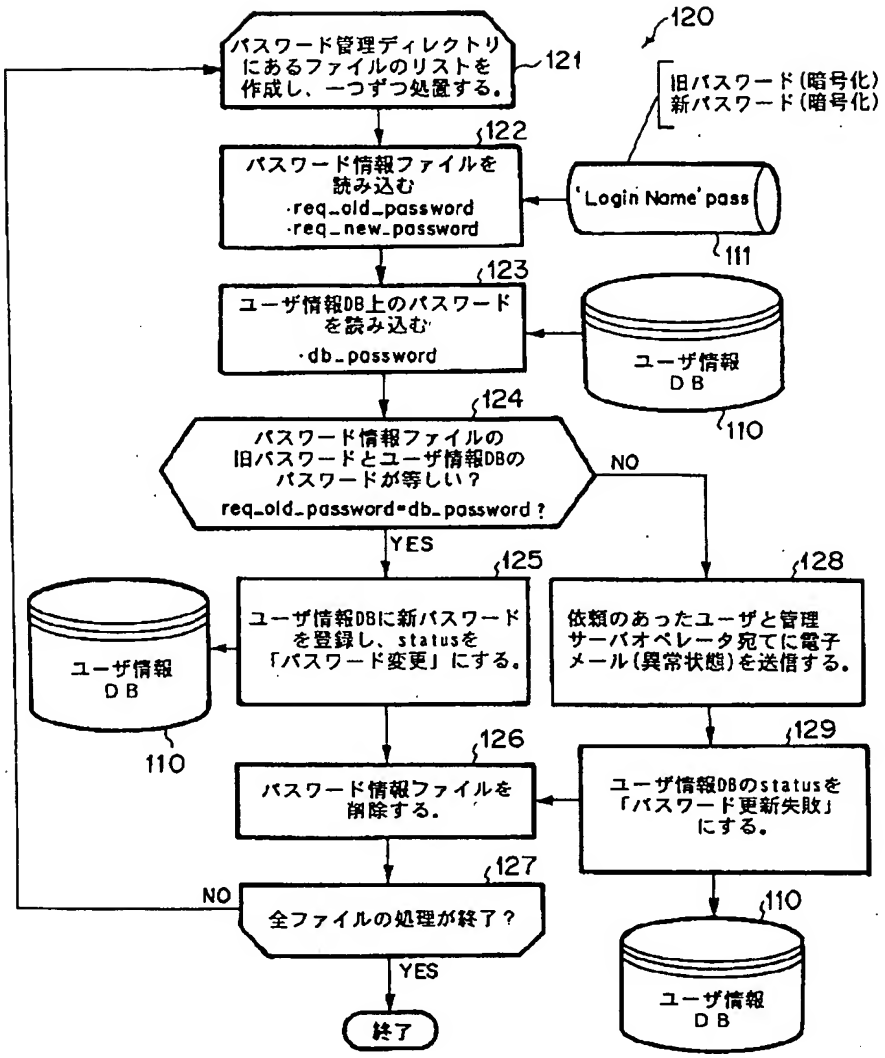
【図1】


100
管理サーバ
110
ユーザ情報DB
120
定時バッチ
パスワード変更
各ユーザから要求があったパスワード変更願いを実行する。
<パスワード変更願い>
ユーザID
変更前パスワード
変更後パスワード
130
定時バッチ
パスワード
更新情報作成
当日に登録されたユーザの情報を各クライアントごとに集計する。集計データは各クライアントごとにファイルへ保管する。更新完了ファイル通知をもってそのファイルを削除する。
140
定時バッチ
更新完了通知確認処理
各クライアントから更新完了通知を確認する。通達があったクライアントからの更新情報は削除する
150
翌日更新時に再び更新
または
運用管理者による強制反映
200
管理クライアント
210
パスワード変更コマンド
変更するパスワードを変更情報登録用ディレクトリに各ユーザID毎に保存する
220
定時バッチ
パスワード変更願い転送
パスワードの変更情報を管理サーバに転送する
230
定時バッチ
パスワード更新
転送してきたユーザ情報に従ってpassword,shadowの変更処理をする。
240
更新完了通知送信
更新完了したことを記したファイルを管理サーバに転送する。
通達なし
転送失敗
転送失敗
転送失敗
(翌日再送)

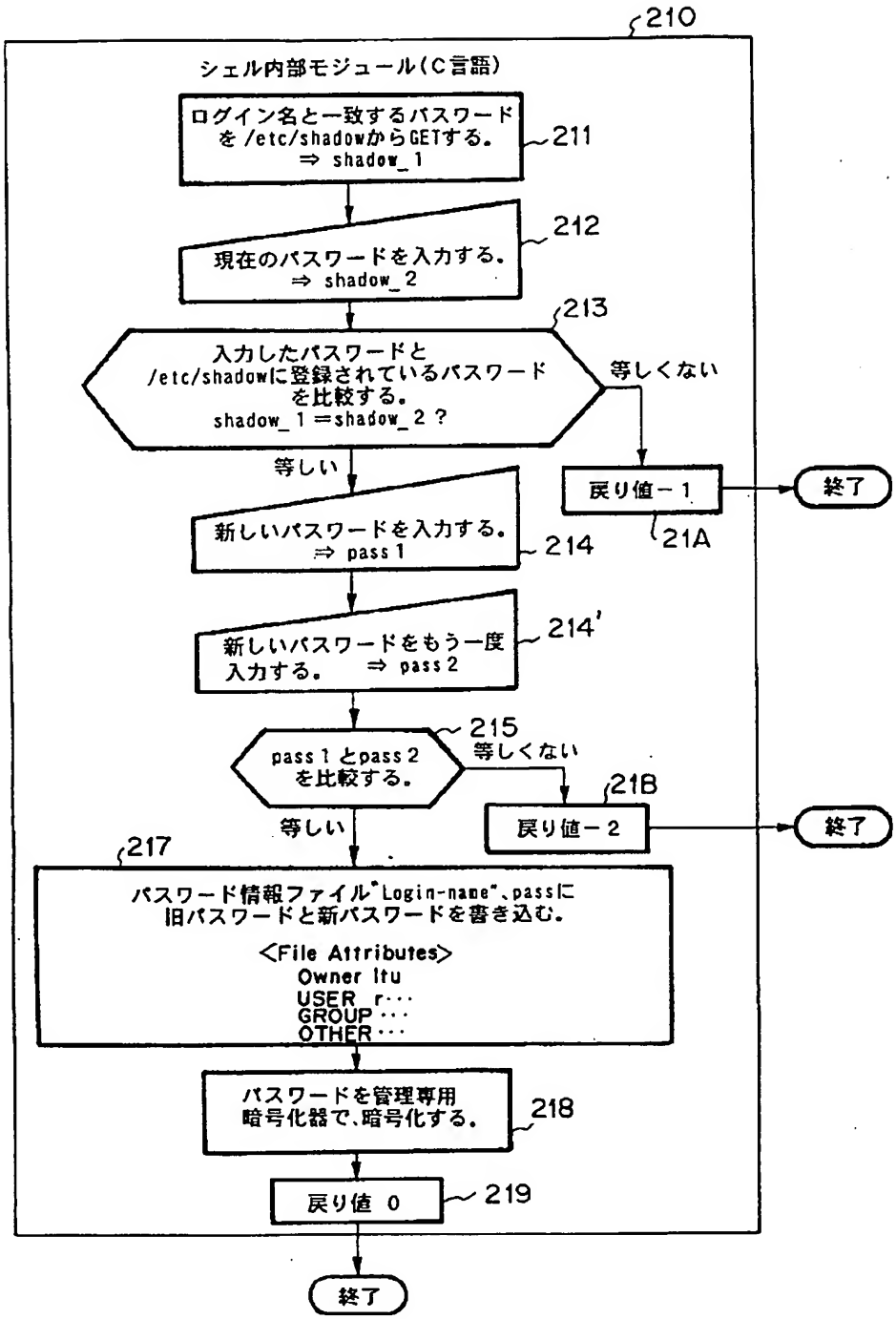
【図2】


100
130
管理サーバ
ユーザ更新情報作成処理
パスワード変更
161
162
ユーザ情報DB上の暗号化(管理専用)されたパスワードを転送用ファイルに書き込む.
ユーザ更新情報を該当する各管理クライアントへ転送する.
163
転送
200
230
管理クライアント
ユーザ情報更新処理
暗号化されたパスワードを複合化する
231
パスワード変更
232
ユーザ情報DBに登録されているパスワードをシステムに反映する.
233
保存
110
ユーザ情報
DB
参照
200
210
管理クライアント
パスワード変更コマンド
211
各管理クライアントのパスワードエントリから暗号化(trypt)されたパスワードを抽出する.
212
ユーザ自身が変更前パスワードを入力する.
213
暗号化されたパスワードと入力したパスワードを比較する.
214
新しいパスワードを2回入力する.
215
パスワード変更願い用ファイルを作成し、暗号化旧パスワードと暗号化新パスワードを保存する.
216
新パスワードを暗号化(管理専用)する.入力した旧パスワードを暗号化(管理用)する.
100
転送
120
管理サーバ
パスワード変更処理
121
パスワード変更願いのファイルを読み込み、暗号化旧パスワードと暗号化新パスワードを読み込む.
122
ユーザ情報DBのパスワードと転送してきた旧パスワードを比較する.
123
新パスワードをユーザ情報DBに登録する.

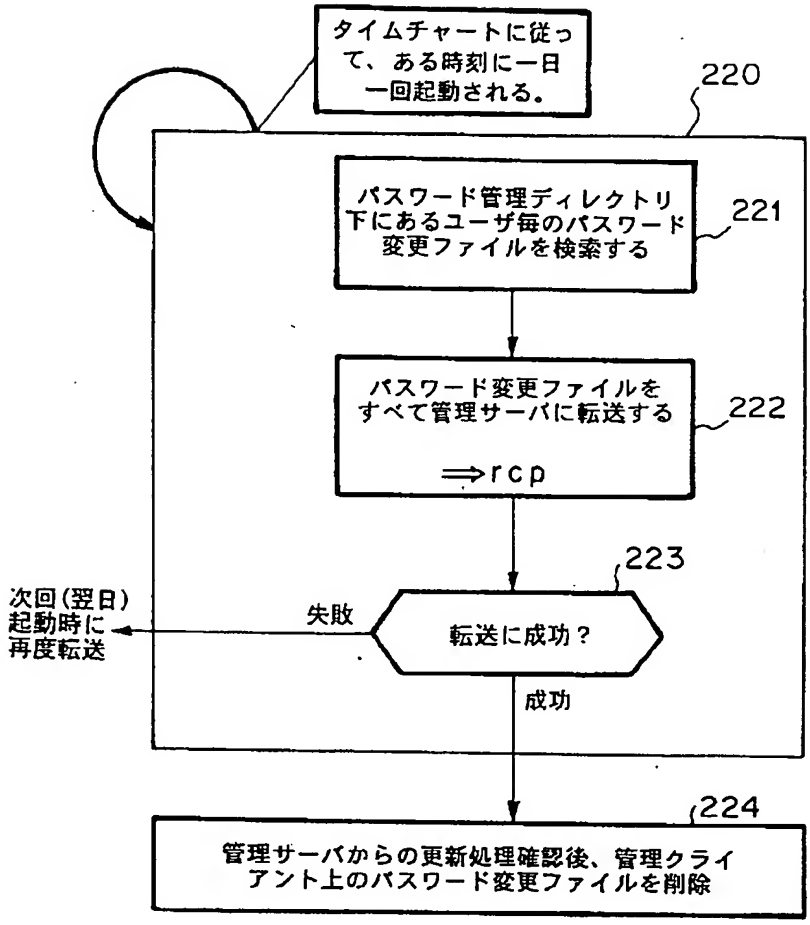
【図3】


パスワード管理ディレクトリにあるファイルのリストを作成し、一つずつ処置する。
121
120
旧パスワード(暗号化)
新パスワード(暗号化)
122
パスワード情報ファイルを読み込む
·req_old_password
·req_new_password
'Login Name' pass
111
123
ユーザ情報DB上のパスワードを読み込む
·db_password
ユーザ情報DB
110
124
パスワード情報ファイルの旧パスワードとユーザ情報DBのパスワードが等しい？
req_old_password=db_password ?
NO
YES
125
ユーザ情報DBに新パスワードを登録し、statusを「パスワード変更」にする。
ユーザ情報DB
110
128
依頼のあったユーザと管理サーバオペレータ宛てに電子メール(異常状態)を送信する。
126
パスワード情報ファイルを削除する。
129
ユーザ情報DBのstatusを「パスワード更新失敗」にする。
127
NO
全ファイルの処理が終了？
YES
終了
110
ユーザ情報DB

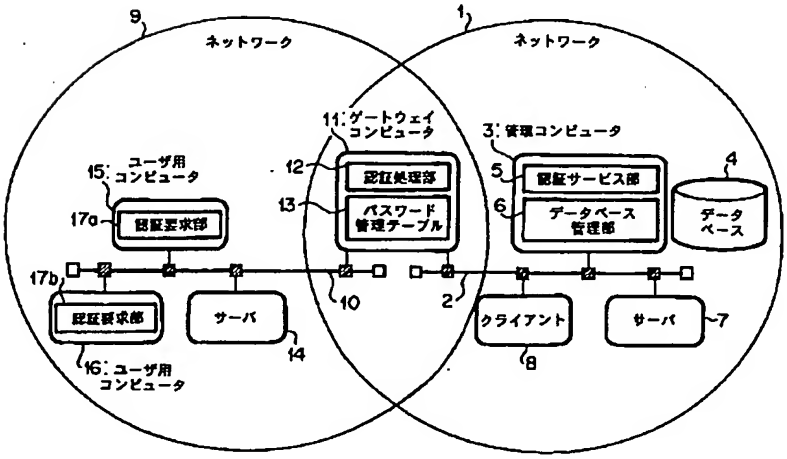
【図4】


210
シェル内部モジュール(C言語)
ログイン名と一致するパスワードを /etc/shadowからGETする。
⇒ shadow_1
211
現在のパスワードを入力する。
⇒ shadow_2
212
213
入力したパスワードと
/etc/shadowに登録されているパスワードを比較する。
shadow_1 =shadow_2 ?
等しくない
等しい
戻り値－1
終了
21A
新しいパスワードを入力する。
⇒ pass1
214
新しいパスワードをもう一度入力する。 ⇒ pass2
214'
215
pass1とpass2を比較する。
等しくない
218
戻り値－2
終了
等しい
217
パスワード情報ファイル"Login-name"、passに旧パスワードと新パスワードを書き込む。
<File Attributes>
Owner Itu
USER r･･･
GROUP ･･･
OTHER ･･･
パスワードを管理専用暗号化器で、暗号化する。
218
戻り値 0
219
終了

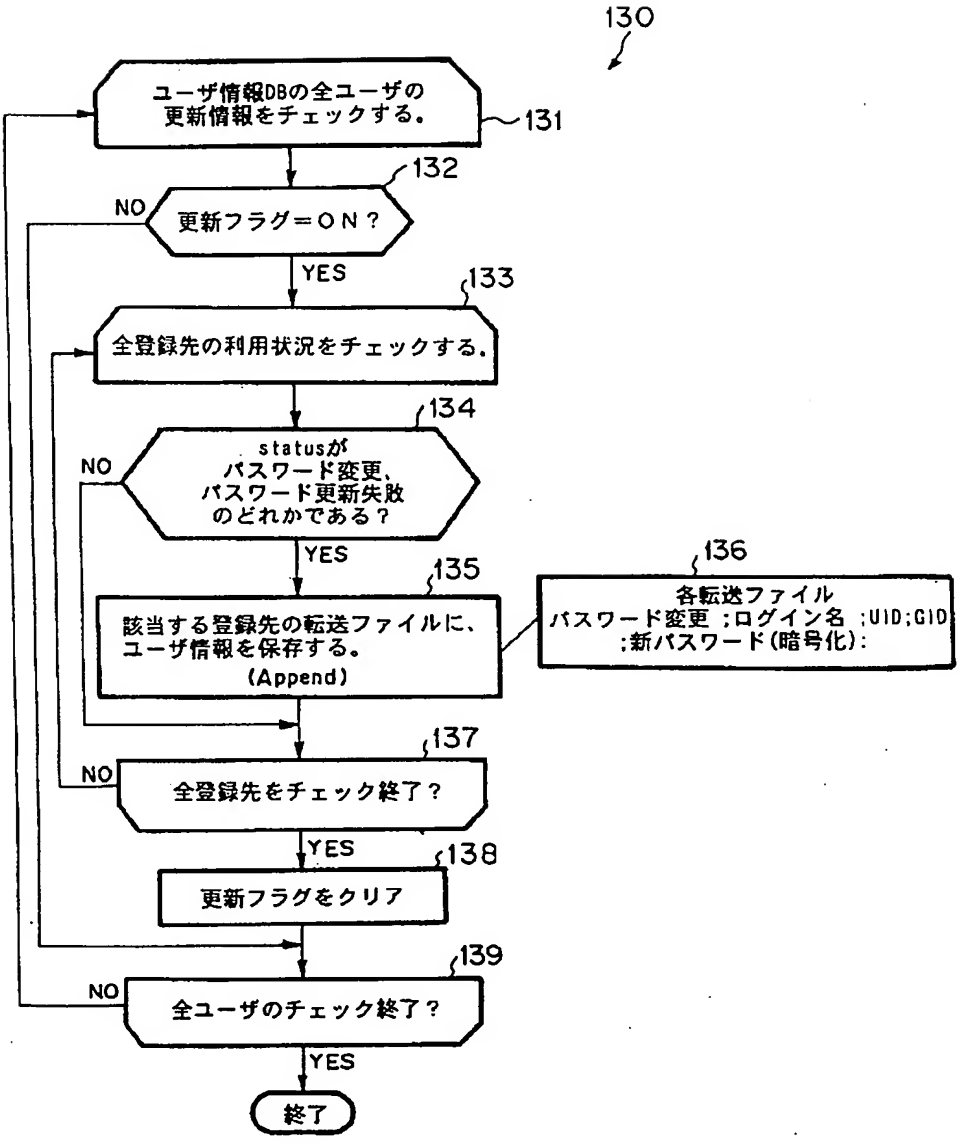
【図5】


タイムチャートに従って、ある時刻に一日一回起動される。
220
パスワード管理ディレクトリ下にあるユーザ毎のパスワード変更ファイルを検索する
221
パスワード変更ファイルをすべて管理サーバに転送する
⇒rcp
222
223
次回(翌日)起動時に再度転送
失敗
転送に成功？
成功
224
管理サーバからの更新処理確認後、管理クライアント上のパスワード変更ファイルを削除

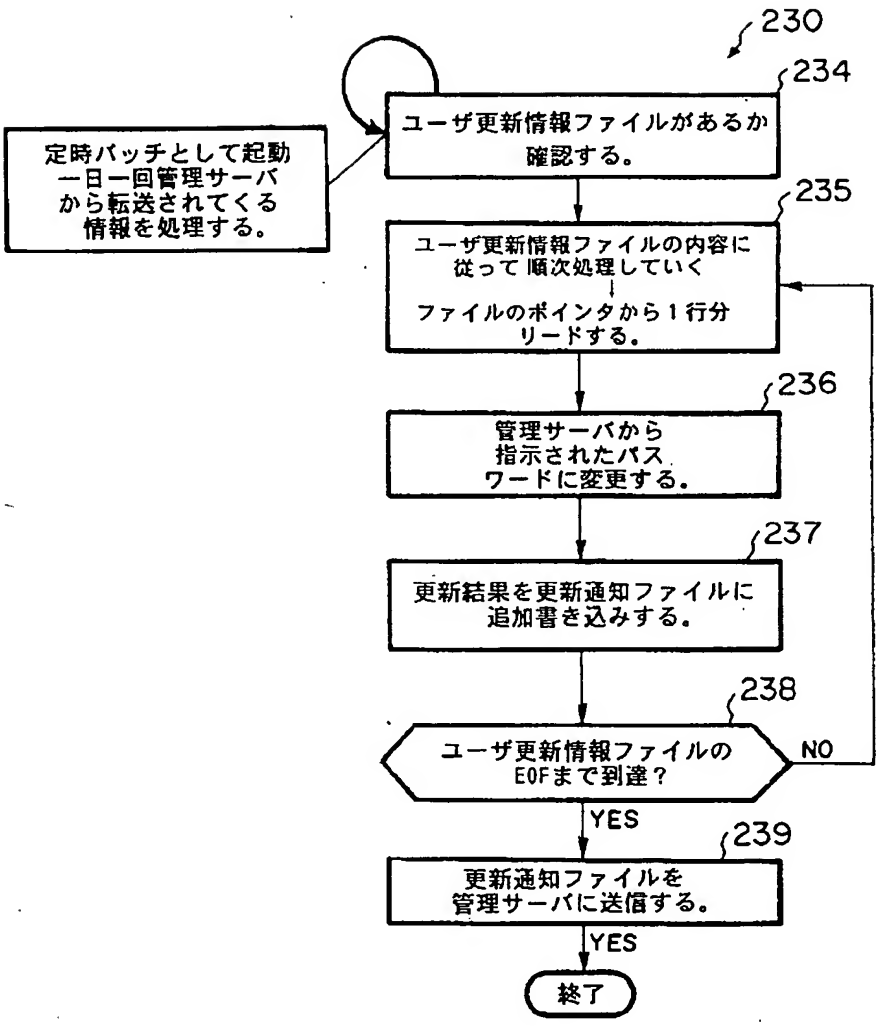
【図8】


9
ネットワーク
1
ネットワーク
11 ゲートウェイコンピュータ
3 管理コンピュータ
15 ユーザ用コンピュータ
12
認証処理部
5
認証サービス部
4
17a
認証要求部
13
パスワード管理テーブル
6
データベース管理部
データベース
17b
認証要求部
サーバ
10
2
クライアント
サーバ
7
14
16 ユーザ用コンピュータ
8

【図6】


130
ユーザ情報DBの全ユーザの
更新情報をチェックする。
131
132
NO
更新フラグ＝ＯＮ？
YES
133
全登録先の利用状況をチェックする。
134
NO
statusが
パスワード変更、
パスワード更新失敗
のどれかである？
YES
135
該当する登録先の転送ファイルに、
ユーザ情報を保存する。
(Append)
136
各転送ファイル
パスワード変更 ;ログイン名 ;UID;GID
;新パスワード(暗号化):
137
NO
全登録先をチェック終了？
YES
138
更新フラグをクリア
139
NO
全ユーザのチェック終了？
YES
終了

【図7】


230
234
ユーザ更新情報ファイルがあるか確認する。
定時バッチとして起動一日一回管理サーバから転送されてくる情報を処理する。
235
ユーザ更新情報ファイルの内容に従って順次処理していく
ファイルのポインタから1行分リードする。
236
管理サーバから指示されたパスワードに変更する。
237
更新結果を更新通知ファイルに追加書き込みする。
238
ユーザ更新情報ファイルのEOFまで到達？
NO
YES
239
更新通知ファイルを管理サーバに送信する。
YES
終了